Digital Forensics Question And Answer

နိုင်ငံတစ်ကာတွင် လက်ခံကျင့်သုံးနေသော နည်းလမ်းများ၊ ISO Standard များကို အခြေခံပြီးရေးသားထားခြင်းဖြစ်ပါသည်။ လက်ရှိမြန်မာနိုင်ငံတွင် စစ်ဆေးရန် အတွက် ဥပဒေ နည်းဥပဒေ တိကျစွာမရှိသေးပါ။ နောင်တစ်ချိန်အတွက်ဖြစ်ပါသည်။

Aung Zaw Myo
www.forensicsmyanmar.com

1/7/2020

Q: Storage Media တွေကို Forensics image လုပ်ရာမှာ အချိန်တူညီနိုင်မလား ?
A: Evidence Device ရဲ့အခြေအနေ၊ Storage Size၊ အသုံးပြုသော နည်းလမ်း နည်းပညာအရ မတူညီနိုင်ပါ။

Q: မူရင်း Evidence Device ရဲ့ Hash Value နဲ့ Forensics image hash Value မတူညီရင် ဘာဖြစ်နိုင်သလဲ ?
A: မူရင်း Evidence Device ရဲ့ Hash Value နဲ့ Forensics image hash Value မတူညီရင် သက်သေခံပျက်ပျယ်ပါတယ်။ စစ်ဆေးရန် စတင်ချိန်မှာ Error ရှိနိုင် ပါ တယ်။

Q: မူရင်း Evidence Device ကို Hash Value မထုတ်ပဲ Forensics image မယူပဲ စစ်ဆေးနိုင်သလား ?
A: Digital Forensics သဘောတရားအရ မှားယွင်းပါတယ်။ ပြဋ္ဌာန်းထားတဲ့ ဥပဒေ၊ နည်းဥပဒေအပေါ်မူတည်ပါတယ်။

Q: Forensics Image ကိုထပ်ပြီး Copy ယူရင် မူရင်း Forensics Image လို့ပြောနိုင်သလား ?
A: ကူးယူတဲ့ Forensics Image က Hash Value မပြောင်းလဲဘူးဆိုရင် မူရင်း Forensics Image အဖြစ်သတ်မှတ်နိုင်ပါတယ်။

Q: စစ်ဆေးတဲ့ နည်းပညာ ပစ္စည်းတွေက အလွယ်တကူသယ်ယူလာနိုင်သလား ?
A: အချို့သော ပစ္စည်းများက အလွယ်တကူသယ်ယူမလာနိုင်ပါ။ သက်သေခံပစ္စည်းကို စစ်ဆေးတဲ့နည်းလမ်းနဲ့ အသုံးပြုတဲ့ ပစ္စည်းအပေါ်မူတည်ပါတယ်။

Q: image တစ်ခုကို Hard Disk, CD , DVD , Etc စတဲ့နေရာများ ကိုရွှေ့ပြောင်း လိုက်ရင်အချက်အလက်Metadataတွေပြောင်းလဲနိုင်လား?
A: image တစ်ခုကို Hard Disk, CD , DVD , Etc ... စတဲ့နေရာများ ကိုရွှေ့ပြောင်းလိုက်ရင် Time နဲ့ပတ်သတ်တဲ့ အချက် အလက်တွေပြောင်း လဲပါသွား ပါတယ်။ ကျန်တဲ့ အချက်အလက်တွေကတော့ image ရဲ့ File Type အပေါ်မူတည်ပါတယ်။

Q: Phone Camera Or Camera က ဓာတ်ပုံတွေရဲ့ Metadata ကို ပြောင်း လဲနိုင်သလား?

A: ဖျက်လို့ရသလို ပြင်ဆင်လို့လဲရပါတယ်။

Q: ပြောင်းရွှေ့လိုက်တဲ့ photo ကို Original လို့ယူဆနိုင်သလား ?

A: Digitally အရမပြောင်းလဲဘူးဆိုရင် Original လို့ယူဆနိုင်ပါတယ်။

Q: Phone (သို့မဟုတ်) ကွန်ပျူတာထဲမှာ ရှိတဲ့ အချက်အလက်တွေက အခြား နေရာ မှာရောရှိနိုင်သလား?

A: အခြားနေရာများမှာလဲ သုံးတဲ့လူအပေါ် သုံးစွဲတဲ့သူရဲ့ Knowledge အရ၊ အခြားသော အခြေအနေများအရ ရှိနေနိုင်ပါတယ်။

Q:Flash Drive တစ်ခုကို စစ်ဆေးရန် Forensically Sound ပြုလုပ်ရင် Flash Drive ထဲမှာရှိတဲ့ File တွေရဲ့ အချက်အလက်တွေ Metadata တွေပြောင်း လဲနိုင် သလား?

A: Flash Drive ထဲမှာရှိတဲ့ File တွေရဲ့ အချက်အလက်တွေ Metadata တွေက Forensically Sound ပြုလုပ်လိုက်ရင် အထဲမှာရှိတဲ့ အချက်အလက် တွေလုံး ဝပြောင်းလဲမသွားပါ။ Forensics Image File ရဲ့ အချက်အလက်ကိုလဲ စစ်ဆေးတဲ့ Process ထဲမှာထည့်သွင်းထားပြီးဖြစ်ပါတယ်။

Q: Expert Witness သည် ဘယ်လိုလူမျိုးကိုသတ်မှတ်နိုင်ပါသလဲ ?

A: သက်ဆိုင်ရာနယ်ပယ်အလိုက် ကျွမ်းကျင်သူကိုသာဆိုလိုပါသည် (ဥပဒေအရ အမျိုးမျိုးသတ်မှတ်နိုင်ပါသည်)

Q:Forensics image နှင့် Clone ကွာခြားချက်ကဘာလဲ ?

A: Forensics Image သည် သက်ဆိုင်ရာ Storage Media အား Bit by Bit ကူးယူထားခြင်းဖြစ်ပါသည် Image မှနေပြီး Recovery ပြုလုပ်နိုင်ပါသည်။။ Clone ပြုလုပ်ခြင်းသည် simulation သဘောသာဖြစ်ပါသည်။

Q:DVR အတွင်းရှိ Hard Disk သည် Computer မှာတပ်ပြီး Edit လုပ်နိုင်ပါသလား ?

A: DVR အမျိုးအစားအပေါ်မူတည်ပြီး ကွန်ပျူတာမှာ DVR Hard Disk ကိုတပ်ပြီး Edit လုပ်လို့ရနိုင်ပါသည်။

Q: **DVR အတွက်သီးသန့်အသုံးပြုရန် သီးသန့် Hard Disk ရှိနိုင်ပါသလား ?**

A: DVR အတွက် သီးသန့် Hard Disk များရှိပါသည်။ သာမန် Hard Disk ထက် Write Time မှာ ပိုပြီးကောင်းမွန်ပါသည်။

Q.CCTV ကိုစစ်ဆေးရာမှာ DVR အတွင်းရှိ Hard Disk ကို တိုက်ရိုက်စစ်ဆေးပါသလား ?

A.တိုက်ရိုက်စစ်ဆေးခြင်းမပြုလုပ်ပါ။ Case အရ သက်ဆိုင်ရာ နာရီအပိုင်းအခြားအလိုက်ကူယူကာ Hash Value ထုတ်ပြီး စစ်ဆေးခြင်း သော်လည်းကောင်း Hard Disk အား Forensics Image ယူကာ (Recovery လုပ်လိုတဲ့အတွက်ကြောင့်) သော်လည်းကောင်း စစ်ဆေးပါသည်။

Q.DVR Hard Disk စစ်ဆေးစဉ် Forensics Image အား Hash Value ထုတ်ယူပါသလား ?

A.စစ်ဆေးစဉ် DVR အတွင်းရှိ Hard Disk ၏ Forensics Image အား Hash Value ထုတ်ယူပါသည်။

Q. Forensics Image အား မည်သည့်အချိန်ထိ သိမ်းဆည်းထားသင့်ပါသလဲ ?

A. ပြဋ္ဌာန်းထားတဲ့ နည်းပညာပိုင်း ဥပဒေမရှိလျှင်တောင်မှ International Standard အရ အမှုပြီးသည် အထိ သိမ်းဆည်းထားသင့်ပါသည်။

Q. DVR အတွင်းရှိ Hard Disk ကို Recovery ယူလို့ရပါသလား ?

A.သတ်မှတ်ထားသော Wipe Time အရ ၁ ကြိမ်ထက်ကျော်ရင် Video File အားလုံးရနိုင်မည်ဟု ထင်မြင်ချက်မပေးနိုင်ပါ။

Q. CCTV စစ်ဆေးရာရမှာ သတိပြုသင့်တဲ့ အချက်အလက်တွေ ရှိပါသလား ကန်သတ်ချက်တွေရှိနိုင်ပါသလား ?

A. တပ်ဆင်ထားသူရဲ့ DVR နဲ့ CCTV အရည်အသွေး။ DVR Setting နဲ့ သိမ်းဆည်းသူ၏ စနစ်ကျမှုသည် ဖိဂ ရာခိုင်နှုန်းရှိပါသည်။

Q.မည်သည့်အချိန်တွင် DVR နှင့်အတူ Hard Disk အားသိမ်းဆည်းသင့်ပါသလဲ ?

Answer

DVR တစ်ခုလုံအား သိမ်းဆည်းရန်လုံလောက်သည်ဟူ ယူဆပြီးသိမ်းယူရမည့် အခြေအနေများမှာ

-DVR အတွင်းမှ Video Record များဖျက်ထားသည်ဟု သံသယရှိလျှင် Timeline View တွင်အပြည့်အစုံမပါဝင်လျှင်

- အခြားအခြေအနေများဖြင့်ဆက်စပ်ရယူရမည့် အနေအထားရှိလျှင်

- အမှုအနေအထားအရ DVR တစ်ခုလုံး သိမ်းဆည်းရမည့်စစ်ဆေးရမည့် အနေအထားရှိလျှင်

- ကူးယူရမည့် Video Size ပမာဏ အရမ်းများနေလျှင်

- ကူးယူဖို့ပြင်ဆင်ရာတွင် (သို့) ကူးယူနေစဉ် နည်းပညာ အခက်အခဲရှိလာလျှင်

- DVR Log တွင် မသင်ကာ စရာ အချက်အလက်တွေ့လာလျှင်

- DVR အား Recovery ပြုလုပ်ရန် လိုအပ်သည်ဟု ယူဆလျှင်

- အခြားသော မသင်္ကာစရာ အချက်အလက်ရှိလာလျှင်

အထက်ပါအချက်များထဲမှအချက်တစ်ချက်နှင့်ညှိစွန်းလာရင်နည်းပညာ သဘောတရားအရ DVR တစ်ခုလုံးအား သိမ်းယူရမည်ဖြစ်ပါသည်။

Q:DVR အတွင်းရှိ Video များ ဘယ်လိုပျက်စီးနိုင်ပါသလဲ ?

A: ရည်ရွယ်ချက်တစ်ခုကြောင့် ပျက်စီးနိုင်ခြေ ၂ ခုရှိပါတယ်။ Storage အား Format ပြုလုပ်ခြင်းနှင့် Video Clip တစ်ခုခြင်းစီအား ဖျက်ထားခြင်းတို့ဖြစ်ပါသည်။ အခြားအကြောင်းကြောင့်ပျက်စီးခြင်းများမှာ သတ်မှတ်ထားချက်အရ Over Write ဖြစ်ခြင်း DVR Firmware ပျက်ခြင်းတို့ဖြစ်ပါတယ်။

Q: DVR ရဲ့ Structure ကိုဘယ်လိုခွဲခြားနိုင်ပါသလဲ ?

A: DVR&HardDisk ပေါင်းစပ်ပြီး ၄ ခုခွဲခြားနိုင်ပါတယ်။ System Information, Data Block Area, Index Information, Free Space

Q: Data Block Area တစ်ခုကို ဘယ်လိုသတ်မှတ်နိုင်လဲ ?

A: Data Block Area ဆိုတာ video ကို Save မည့် File System နဲ့ Hard Disk Size အပေါ်မူတည်ပြီး သတ်မှတ်ထားနိုင်ပါတယ်။

Q: Block တစ်ခုချင်းမှာ Channel ဘယ်လောက်ပါနိုင်သလဲ ?

A:Block တစ်ခုခြင်းကို CCTV channel တစ်ခုသာသတ်မှတ်နိုင်ပြီး Block နံပတ်နဲ့ CCTV Channel မူတူညီနိုင်ပါ။ ဥပမာ Block 1 = Channel1 Block 2 = Channel 2 Block 3 = Channel 3 Block 4 = Channel 2 ဖြစ်သွားနိုင်ပါတယ်။

Q: Index ဆိုတာဘာလဲ ?

A: အစပိုင်း record တွေက ထိပ်ဆုံး Block မှာရှိနေပြီး နောက်ဆုံး Record တွေက Block အောက်ဆုံးမှာ ရှိနေပါတယ်။ အဲဒီ Block တွေကို Index မှာမှတ်သားထားပါတယ်ပြန်လည်ကြည့်ဖို့ လွယ်ကူအောင်ပြုလုပ်ပေးပါတယ်။

Q: Overwrite လုပ်ရင်ဘယ်လိုဖြစ်နိုင်သလဲ ?

A: Overwrite လုပ်ရင် အစောတုန်းက စစခြင်း Record လုပ်တဲ့ အစပိုင်း Block တွေက အောက်ကိုရောက်ရှိသွားပြီး နောက်ထပ် Video ကအပေါ်ကိုရောက်ရှိ သွားပါတယ်။

Q: Format လုပ်လိုက်ရင် ဘယ်လိုဖြစ်သွားသလဲ ?

A: Format ပြုလုပ်လိုက်ရင် မှတ်သားထားတဲ့ အစ Block နဲ့ အဆုံး Block တွေကို Index ကနေဖျက်လိုက်ပါတယ်။ဒါကြောင့် Video တွေကို View ကနေ ကြည့်လို့ရနိုင်မှာ မဟုတ်ပါဘူး။ ဒါပေမဲ့ Format လုပ်လိုက်တဲ့ Hard Disk ပေါ်မှာ data တွေက အဲဒီ Hard Disk အပေါ်ကို Overwrite မလုပ်မခြင်း ရှိနေပါတယ်။

Q: Format ချပြီး Overwrite ပြုလုပ်ခဲ့ရင် အရင် Video တွေပြန်ရနိုင်ချေရှိလား ?
A: အခြေအနေအရ Frame Level အထိ Recovery ပြုလုပ်ရပါမယ်။အပြည့်အဝ ရနိုင်ချေမရှိပါ။

Q: DVR အတွင်းမှ Video Clip များကို ပြန်လည်ရယူဖို့ အချိန်မည်မျှလိုအပ်ပါသလဲ
A:DVR hard Disk အခြေအနေ၊ ပမာဏ အပေါ်မူတည်ပါသည်။ အတိအကျ မပြောဆိုနိုင်ပါ။

Q: Mobile ဖုန်းသည် အနီးဆုံး ဆက်သွယ်ရေးတာဝါတိုင်ကို ချိတ်ဆက်တာလား ?
A: Mobile ဖုန်းသည် Signal အကောင်းဆုံး ဆက်သွယ်ရေးတာဝါတိုင်ကို ချိတ်ဆက်ပါသည်။

Q: Call Detail Record (CDR) ထဲတွင် Mobile Phoneတည်နေရာ ပါဝင်ပါသလား ?
A: Call Detail Record (CDR) ထဲတွင် Mobile Phone တည်နေရာ မပါဝင်ပါ။ ဆက်သွယ်ရေးတာဝါတိုင်၏ တည်နေရာသာပါဝင်ပါသည်။

Q: Telecom မှ ပေးသော ဖုန်းတည်နေရာသည် တိကျပါသလား ?
A: မတိကျနိုင်ပါ။ Case ပေါ်မူတည်ပြီး CDR File အပါအဝင် Telecom မှ အခြားသော အချက်အလက် 5 ခုမှ 13 ခု အတွင်းပြန်လည်တွက်ချက်ရပါမည်။

Q: Call Detail Record (CDR) တွက်ချက်စစ်ဆေးမှုတွင် Industry Standard ရှိပါသလာ ?
A: Call Detail Record (CDR) တွက်ချက်စစ်ဆေးမှုတွင် Industry Standard ရှိပါသည်။

Q: Call Detail Record (CDR) စစ်ဆေးရာမှာ စစ်ဆေးသူက မသမာမှု ပြုလုပ်နိုင်ချေရှိသလား ?
A: မပြုလုပ်နိုင်ပါ။ Call Detail Record (CDR) စစ်ဆေးရာမှ သက်ဆိုင်ရာ

Telecom တွင် မူရင်း CDR File နှင့် ပတ်သတ်သောမူရင်း အချက်အလက်များ ရှိပါသည်။

Q: CDR,IPDR Record ကို Telecom တွေက ဘယ်အချိန်ထိ သိမ်းထားသလဲ ?
A: နိုင်ငံ၏ ဥပဒေပေါ်သာ မူတည်ပါသည်။ အချို့နိုင်ငံများတွင် ၃လ ၆လ ၁နှစ် မှ ၃ နှစ်အထိ ထိန်းသိမ်းထားပါသည်။

Q: Call Detail Record ကနေဘာတွေတွက်ချက်နိုင်လဲ ?
A: ဘယ်နေ့ ဘယ်အချိန်မှာ ရှိနေလဲ ဆိုတဲ့ ယေဘူယျတည်နေရာ (latitude and longitude)
A: ဘယ်နေ့ ဘယ်အချိန်မှာ နေရာမှာ မရှိနိုင်ဘူးဆိုတဲ့ (latitude and longitude)
A: ဖုန်နဲ့အတူ အခြားဘယ်သူတွေရှိနိုင်တယ်၊ အတူရှိနေနိုင်တယ်
A: ဘယ်အချိန်မှာ ဘယ်နေရာတွေကို သွားခဲ့တယ်ဆိုတဲ့ Call Route မှတ်တမ်း
A: ဘယ်ရက် ဘယ်အချိန်မှာ ဘယ်သူတွေနဲ့ ဆက်သွယ်ခဲ့တယ်ဆိုတဲ့ မှတ်တမ်း
A: IPDR ကနေ အင်တာနက်အသုံးပြုမှုမှတ်တမ်း၊

Q: Mobile Forensics နဲ့ CDR ဆက်စပ်ပါသလား ?

A: Some Cases များအတွက် ဖုန်းကနေ စစ်ဆေးလို့ရရှိတဲ့ အချက်အလက်နဲ့ Telecom ကနေရရှိသော အချက်အလက်များကို တွက်ချက်ပြီး တိုက်ဆိုင်ဖို့လိုအပ်ပါတယ်။

Q: Phone Location ကို ဘာကို အဓိက ထားတွက်ချက်လဲ ?
A: Cell Site ရဲ့ Sector ပေါ်ကို အဓိကထားပြီးတွက်ချက်ပါတယ်။
(latitude , longitude and azimuth)

Q: ပထမဆုံး Cell Tower ကို ဖုန်းကနေ Network အရရွေးချယ်ပါသလား ?
A: ပထမဆုံး Cell Tower ကို ဖုန်းကနေပဲ ရွေးချယ်ပါတယ်။

Q: CDR Mapping အတွက်အသုံးပြုသော Application များမှ ရရှိသော အဖြေသည် တိကျပါသလား ?
A: Mapping ပြုလုပ်ရာတွင် ပိုပြီး တိကျနိုင်စေရန် လူ၏ တွက်ချက်မှုပါ အသုံးပြုပါသည်။ သက်ဆိုင်ရာ မြေပုံရဲ့ Terrain အနေအထားအရဖြစ်ပါသည်။

Q: Telecom မှရရှိသော အချက်အလက်အပြင် ဘယ်နေရာနေ ဖုန်းနဲ့ပတ်သတ်သော အချက်အလက်များရရှိနိုင်ပါသလဲ ?

A: သက်ဆိုင်ရာ Law Enforcement ကနေ Google မှ GEOFENCE SEARCH WARRANT နည်းဖြင့် ဖုန်းနဲ့ပတ်သတ်သော အချက်အလက်များကို ရရှိနိုင်ပါသည်။